Dorota Łażewska
Wyższa Szkoła Gospodarki Euroregionalnej
im. Alcide De Gasperi w Józefowie
tales.ratio@wp.pl

JOURNAL OF MODERN
SCIENCE TOM 4/31/2016,
S. 431–442

IX Scientific Conference Modern Information Technology and countering security threats National Centre for Nuclear Research 18 October 2016

IX Ogólnopolska Konferencja Naukowa „Nowoczesne narzędzia informatyczne w przeciwdziałaniu zagrożeniom bezpieczeństwa"

Wyższa Szkoła Gospodarki Euroregionalnej im. Alcide De Gasperi w Józefowie Narodowe Centrum Badań Jądrowych w Świerku 18.10.2016 r.

18 października 2016 r. w Narodowym Centrum Badań Jądrowych w Świerku odbyła się IX Ogólnopolska Konferencja Naukowa „Nowoczesne narzędzia informatyczne w przeciwdziałaniu zagrożeniom bezpieczeństwa". Została ona zorganizowana przez Wyższą Szkołę Gospodarki Euroregionalnej im. Alcide De Gasperi w Józefowie oraz Narodowe Centrum Badań Jądrowych w Świerku. W tym naukowym spotkaniu udział wzięło liczne grono naukowców, ludzi biznesu, przedstawicieli służb publicznych i organów administracji państwowej oraz pracowników ośrodków badawczych specjalizujących się w tworzeniu nowoczesnych narzędzi informatycznych.

Niniejsze wydarzenie naukowe to kolejna inicjatywa uczelni Alcide De Gasperi, która już po raz dziewiąty zaproponowała debatę nad zasadniczymi problemami wynikającymi z zagrożenia bezpieczeństwa – tej uniwersalnej potrzeby ludzkiej, niezależnej od czasu i przestrzeni. W czasach „płynnej ponowoczesności" XXI w. jest to zaś szczególnie istotny temat naukowej refleksji. Człowiek współczesny jest bowiem zanurzony w nowej czasoprzestrzeni, swoistym „żywiole", czyli cyberprzestrzeni, miejscu wielu możliwości budowania strategii bezpieczeństwa przy wykorzystaniu nowoczesnych narzędzi informatycznych identyfikujących wiele starych i nowych zagrożeń. Nad

różnorodnymi problemami ulokowanymi w cyberprzestrzeni, mającymi zaś konsekwencje w świecie realnym, debatowali zatem zaproszeni goście.

Współorganizatorem konferencji był Uniwersytet Rzeszowski, Wyższa Szkoła Policji w Szczytnie, Urząd do spraw Cudzoziemców, Klub Nowej Gospodarki Powiatu Otwockiego oraz Centrum Naukowo-Badawcze Ochrony Przeciwpożarowej – Państwowy Instytut Badawczy w Józefowie. Patronat honorowy nad konferencją objęli: Biuro Bezpieczeństwa Narodowego, Główny Inspektorat Sanitarny, Państwowa Inspekcja Sanitarna, Krajowa Izba Gospodarki Cyfrowej, Związek Miast Polskich, Stowarzyszenie Chrześcijańskich Przedsiębiorców „Nostra Res", Stowarzyszenie Informatyków Polskich, Straż Graniczna oraz Centrum Naukowo-Badawcze Ochrony Przeciwpożarowej – Państwowy Instytut Badawczy w Józefowie.

Czas konferencyjnych obrad został podzielony na kilka zasadniczych części: wykład wprowadzający, panel dyskusyjny oraz równoległe sesje tematyczne.

Uroczystego otwarcia konferencji dokonał **prof. dr hab. Bronisław Sitek** (Uniwersytet Humanistycznospołeczny w Warszawie; WSGE im. Alcide De Gasperi). Witając zgromadzonych gości, Profesor podkreślił priorytetową rolę bezpieczeństwa, które wśród najbardziej cenionych wartości jest dziś wymieniane na pierwszym miejscu, nawet przed tak upragnionym powszechnie dobrem, jakim jest wolność. W imieniu Dyrekcji Narodowego Centrum Badań Jądrowych w Świerku, na którego terenie odbywała się konferencja, wystąpił **prof. dr hab. Wojciech Wiślicki**, życząc uczestnikom konferencji owocnych obrad w tak szczególnym miejscu, jakim jest Narodowe Centrum Badań Jądrowych, jedyna tego typu placówka w Polsce. Ośrodek ten to swoisty symbol konieczności troski o bezpieczeństwo informatyczne i jak żadne inne miejsce może ulec różnego rodzaju zagrożeniom.

W imieniu Wyższej Szkoły Gospodarki Euroregionalnej im. Alcide De Gasperi w Józefowie zgromadzonych gości powitał **Rektor – Jego Magnificencja dr Tadeusz Graca**. Wychodząc od faktu powszechnego zastosowania technologii informatycznych, podkreślił konieczność pogłębionego namysłu nad zagrożeniami generowanymi przez owe technologie. Wielowymiarowe i skomplikowane zagrożenia wskazują na etyczny problem podwójnego skutku. Pierwszym skutkiem, zamierzonym przez twórców technik informatycz-

nych, jest ich wykorzystanie dla społecznego dobra. Drugim skutkiem (niezamierzonym) jest zaś możliwość wykorzystania tego narzędzia do celów, których osiągnięcie zagraża bezpieczeństwu w cyberprzestrzeni, w dalszej kolejności wpływa zaś na jakość życia w świecie realnym. W związku z tym faktem wydaje się, iż naukowa analiza poświęcona sposobom działania technik informatycznych jest nieodzownym „znakiem czasu".

Wykład wprowadzający wygłosił **prof. nadzw. dr hab. inż. Marek Kisiel-Dorohinicki** z Akademii Górniczo-Hutniczej im. Stanisława Staszica w Krakowie, analizując „Możliwości i perspektywy zastosowania dedykowanych narzędzi analitycznych w obszarze bezpieczeństwa publicznego". Profesor skonfrontował ze sobą dwa typy analizy jako procesu porządkowania rzeczywistości. Pierwsza z nich to analiza wykonywana przez nowoczesne dedykowane narzędzia analityczne. Dzięki nim można pozyskiwać, gromadzić oraz przechowywać informacje. Jednak są one nieuporządkowane i zbyt różnorodne. Na tym etapie pozostają bezkształtną masą danych. Dopiero ludzka mądrość, czyli drugi rodzaj analizy prowadzonej przez człowieka, nie zaś przez maszynę, pozwala na ich zrozumienie i podjęcie odpowiednich decyzji. Dlatego też w „piramidzie wiedzy" nie może zabraknąć (obok takich elementów, jak dane, informacje i wiedza) ludzkiej mądrości. Przekształcanie uzyskanych przez maszynę danych w informacje oraz wiedzę będzie wtedy skuteczne.

Po wykładzie odbył się panel dyskusyjny „Zastosowanie nowoczesnych technologii informatycznych i elektronicznych dla zapewnienia bezpieczeństwa". W trakcie tej części obrad, prowadzonych przez **dr. inż. Pawła Chodaka**, postawiono wiele pytań, udzielając różnorodnych odpowiedzi, dlatego też mottem tego spotkania była sentencja: „Cyberbezpieczeństwo – wiele pytań i odpowiedzi – wspólny cel". Uczestnicy panelu dokonali analizy stanu bezpieczeństwa informatycznego z perspektywy zasadniczych organów państwowych jako kluczowych podmiotów w strategii zapewnienia bezpieczeństwa zarówno regionalnego, jak i narodowego tej części Europy.

W panelu dyskusyjnym głos zabrali: Ireneusz Przeklasa – Dyrektor Biura Informatyki Urzędu do spraw Cudzoziemców; płk SG Mariusz Kijowski – Zastępca Dyrektora Biura Łączności i Informatyki Komendy Głównej Straży Granicznej; bryg. dr inż. Dariusz Wróblewski – Dyrektor Centrum Naukowo-Badawczego Ochrony Przeciwpożarowej – Państwowy Instytut Badawczy

w Józefowie; dr Jacek Gajewski – Kierownik Działu Badań i Współpracy Międzynarodowej w Narodowym Centrum Badań Jądrowych w Świerku; Marek Posobkiewicz – Główny Inspektor Sanitarny Kraju; Tomasz Andrukiewicz – Prezydent Miasta Ełk oraz przedstawiciel Związku Miast Polskich; gen. bryg. rez. Włodzimierz Nowak – pełnomocnik Ministra Cyfryzacji ds. cyberbezpieczeństwa, Dyrektor Departamentu Cyberbezpieczeństwa w Ministerstwie Cyfryzacji oraz Zsolt Tadeusz Fekete – Prezes Zarządu Algotech Polska sp. z o.o., absolwent Canadian Executive MBA.

Ireneusz Przeklasa scharakteryzował specyfikę pracy Urzędu do spraw Cudzoziemców, który zapewnia wielowymiarową pomoc przy legalizacji pobytu, udzielając ochrony cudzoziemcom przebywającym w granicach Rzeczypospolitej Polskiej. I właśnie za pomocą narzędzi informatycznych urząd ten może wspierać proces przemieszczania się cudzoziemców, analizując przy tym najnowsze trendy, zjawiska i tendencje w tym obszarze oraz wpływając dzięki temu na bezpieczeństwo kraju. Należy dodać, iż jakość dokumentów wydawanych przez urząd cudzoziemcom jest na światowym poziomie. Urząd wyprzedza zatem zobowiązania podjęte wobec Unii Europejskiej. Gwarancją bezpieczeństwa jest jednak zawsze człowiek. Jeżeli bowiem zawiedzie czynnik ludzki, żadne systemy bezpieczeństwa nie będą skuteczne. Z kolei **płk SG Mariusz Kijowski** wskazał na zagrożenia specyficzne dla terenów granicznych. Wymienił wśród nich fakt nielegalnego przekraczania granic, trudności w identyfikacji osób, podrabianie dokumentów oraz zjawisko kradzieży tożsamości. W kontekście owych zagrożeń niezastąpioną funkcję pełnią zatem technologie informatyczne, przy pomocy których można wykryć nielegalne dokumenty paszportowe czy wykonać badania biometryczne, usprawniając system odpraw granicznych. **Bryg. dr inż. Dariusz Wróblewski** omówił natomiast wkład projektów badawczych, realizowanych przez Centrum Naukowo-Badawcze Ochrony Przeciwpożarowej – Państwowy Instytut Badawczy w Józefowie, w zapewnienie bezpieczeństwa państwa polskiego w zakresie ochrony przeciwpożarowej oraz zarządzania antykryzysowego. Z kolei **dr Jacek Gajewski**, reprezentując Narodowe Centrum Badań Jądrowych w Świerku, na terenie którego znajduje się reaktor „Maria", scharakteryzował nowe technologie używane dla zapewnienia bezpieczeństwa układów nuklearnych oraz omówił działanie programowalnych sterowników

logiczno-cyfrowych PLC. Tematykę bezpieczeństwa zdrowotnego zaprezentował **Marek Posobkiewicz** – Główny Inspektor Sanitarny Kraju. Podkreślił, iż duży zbiór danych, dostępny przy pomocy technologii informatycznych, będzie jedynie „pustym naczyniem", jeżeli osobom, które korzystają z tych danych, zabraknie mądrości. Natomiast wiedza i mądrość, przy udziale nowoczesnych technologii informatycznych, może przyczyniać się między innymi do wczesnego ostrzegania o wielu niebezpieczeństwach. Wykrycie toksycznych substancji w produktach spożywczych czy zatrzymanie na granicy szkodliwych partii żywności jest jedynie końcowym efektem działań ludzkiej mądrości oraz zaawansowanych technologicznie narzędzi informatycznych. **Tomasz Andrukiewicz** – Prezydent Miasta Ełk oraz przedstawiciel Związku Miast Polskich przedstawił kwestie bezpieczeństwa z perspektywy urzędów państwowych. Prawie każdego dnia są bowiem przeprowadzane ataki hakerskie na systemy samorządowe gromadzące wrażliwe dane, niezbędne do wydawania decyzji administracyjnych. W związku z tym system zabezpieczeń jest tu sprawą priorytetową. Przykładem wdrożenia nowoczesnych zabezpieczeń informatycznych może być Miasto Ełk. W 2006 r. posiadało osiem kamer analogowych. W 2016 r. dysponuje już trzystoma kamerami cyfrowymi. Ponadto stosuje, zamiast zabezpieczeń sieci lokalnych, zaawansowaną technologicznie centralną serwerownię oraz centralnie sterowane oświetlenie miasta. W imieniu Ministerstwa Cyfryzacji wystąpił **gen. bryg. rez. Włodzimierz Nowak** – pełnomocnik Ministra Cyfryzacji ds. Cyberbezpieczeństwa. Zwrócił uwagę na fakt, iż zasadniczym sposobem myślenia o obronie przed cyberzagrożeniem generującym cyberwojnę jest współpraca wielu systemów. Ten sposób myślenia jest założeniem modelu będącego podziałem systemów sieciowych współpracujących ze sobą w ściśle określony sposób (model OSI). Chodzi zaś o to, aby ludzie, procedury i technologie współpracowali ze sobą. Wpierw jednak wagę bezpieczeństwa w cyberprzestrzeni muszą zrozumieć menedżerowie oraz informatycy, którzy przywiązują zbyt dużą wagę do architektury owych narzędzi, nie zaś do ich bezpieczeństwa. Nie mniej istotne jest budowanie świadomości użytkowników (wręcz od przedszkola), gdyż ok. 15 milionów komputerów jest zainfekowanych. Kolejną kwestię stanowi uspójnienie procedur. Jeśli chodzi o technologie, to trzeba opracować system wczesnego ostrzegania, aby zabezpieczyć się przed atakiem prowadzo-

nym zwykle przez wielu operatorów. **Zsolt Tadeusz Fekete** – Prezes Zarządu Algotech Polska sp. z o.o. – omawiając relacje cyberprzestrzeni z biznesem, zwrócił uwagę na taki czynnik ochrony przed zagrożeniami, jakim jest ludzka mądrość, ponieważ każdy system będzie dobry, pod warunkiem jednak że będzie z niego korzystał człowiek wyposażony nie tylko w wiedzę z zakresu techniki, lecz również w kompetencję mądrości.

Po zakończeniu panelu dyskusyjnego odbyła się sesja tematyczna „Bezpieczeństwo informatyczne instalacji przemysłowych oraz systemów informatycznych urzędów państwowych i samorządowych" prowadzona przez dr. hab. Pawła Sobkiewicza – Dyrektora Parku Naukowo-Technologicznego Narodowego Centrum Badań Jądrowych. Wprowadzeniem w szczegółową problematykę sesji był wykład **Pawła Sobkiewicza** *Bezpieczeństwo w złożonym świecie*, ukazujący kategorię ryzyka jako szerszego kontekstu społeczno-cywilizacyjnego funkcjonowania nowoczesnych technologii informatycznych. Konkluzją wykładu może być teza, iż ocena ryzyka i metody zapewnienia bezpieczeństwa są niepełne i niepewne. „Chcemy [bowiem] przewidzieć nieprzewidywalne".

Płk rez. mgr inż. Krzysztof Cygańczuk (z Centrum Naukowo-Badawczego Ochrony Przeciwpożarowej – Państwowy Instytut Badawczy w Józefowie) przybliżył znaczenie bezzałogowych statków powietrznych w zapewnieniu bezpieczeństwa wewnętrznego i ochrony ludności. Przygotowaniem kadry kierowniczej, wyspecjalizowanej w obsłudze tego typu statków, zajmuje się Centrum Szkoleniowe Systemów Bezzałogowych przy Państwowym Instytucie Badawczym w Józefowie, który działa już od 40 lat. Jednak wykorzystanie różnorodnych statków bezzałogowych (wirnikowych czy płatowych) to nie tylko same korzyści. Możliwe są bowiem zagrożenia ze strony omawianych urządzeń, szczególnie w trakcie imprez masowych: powodowanie chaosu, zrzucanie niebezpiecznych ładunków i odwracanie uwagi służb publicznych.

Kolejny referat *Cyberbezpieczeństwo w sieciach przemysłowych* wygłosił **prof. nadzw. dr hab. Krzysztof Szczypiorski** z Politechniki Warszawskiej i Krajowej Izby Gospodarki Cyfrowej. Punktem wyjścia refleksji na temat cyberprzestrzeni było odniesienie do czterech żywiołów świata. Cyberprzestrzeń jest bowiem kolejnym żywiołem. Przy czym jako nowy żywioł, wchodząc w pozostałe, nie daje się w sposób precyzyjny wydzielić. Nazwa

owej przestrzeni została wybrana przypadkowo przez W. Gibsona, amerykańskiego pisarza literatury science fiction, utrwalając się na stałe w terminologii medialnej i naukowej. Profesor poruszył temat systemu informatycznego SCADA, w którym brak polityki zabezpieczeń. Sieciom przemysłowym może zagrażać Stuxnet, który przeprogramowuje instalacje przemysłowe, cyberatak Duqu czy najbardziej zaawansowany robak Flame wykradający dane przechowywane w pamięci komputerów.

Tematyka kolejnych dwóch prezentacji została skoncentrowana wokół problematyki bezpieczeństwa energetycznego. W referacie *Niezależna wyspa energetyczna w oparciu o OZE i magazyny energii a cyberbezpieczeństwo energetyczne* **Roman Trzaskalik** – Prezes Parku Naukowo-Technologicznego „Eko-Centrum" w Katowicach oraz Prezes Stowarzyszenia „Nostra Res" – omówił działalność „niezależnej wyspy energetycznej", demonstracyjnych instalacji fotowoltaicznych i Laboratorium Inteligentnych Sieci. „Eko-Centrum" to bowiem miejsce gromadzące przedsiębiorców, naukowców i inwestorów, którzy łącząc biznes z nauką, tworzą technologie i usługi z zakresu energooszczędności. **Prof. dr hab. inż. Konrad Świrski** z Politechniki Warszawskiej/Prezes Transition Technologies S.A. w temacie *Zagadnienia cyberbezpieczeństwa infrastruktury krytycznej w energetyce* zwrócił uwagę na prostotę, a zarazem powagę owej refleksji, twierdząc, iż chciałby pokazać, „jak można wyłączyć światło". Infrastruktura krytyczna to różne obiekty niezbędne do funkcjonowania gospodarki państwa. To dzięki nim ludność kraju jest zaopatrzona w energię, surowce energetyczne i paliwa, żywność i wodę, z możliwością wzajemnej komunikacji. Zapewnienie bezpieczeństwa owej strukturze wymaga ciągłej zmiany myślenia, aby w miarę skutecznie wykrywać wciąż nowe sposoby wojny informatycznej, poszukując nowoczesnych strategii obrony zgodnie z zasadą „kopania dołów" lub/i „stawiania murów".

W dalszej części konferencji **Grzegorz Staniszewski** – naczelnik Wydziału Prewencji i Profilaktyki Straży Miejskiej m.st. Warszawy – przybliżył strategie działania Straży Miejskiej na przykładzie jednostki stołecznej. Wykład *Monitoring zagrożeń w miastach. Działania Straży Miejskiej m.st. Warszawy w zakresie bezpieczeństwa i porządku publicznego na rzecz społeczności lokalnej* stał się okazją do prezentacji zintegrowanego systemu zarządzania i ko-

ordynacji niniejszych służb (interweniujących co 10 minut) w celu ochrony spokoju i porządku, kontroli ruchu drogowego, zabezpieczenia imprez masowych, zapewnienia bezpieczeństwa dzieciom i młodzieży czy wykonywania patroli ekologicznych.

Oprócz panelu dyskusyjnego oraz sesji plenarnej odbyły się równoległe sesje tematyczne: „Nowe technologie w kontekście bezpieczeństwa zdrowotnego" (prowadzenie: **prof. dr hab. Józef Knap**/Warszawski Uniwersytet Medyczny); „Cyberbezpieczeństwo w praktyce" (prowadzenie: **prof. dr hab. Stanisław Sagan**/Uniwersytet Rzeszowski) oraz dwie części sesji „Współczesne zagrożenia bezpieczeństwa narodowego Polski" (cz. I prowadzenie: **prof. nadzw. dr hab. Sławomir Zalewski**/Wyższa Szkoła Policji w Szczytnie; cz. II prowadzenie: **dr Krzysztof Krassowski**/WSGE im. Alcide De Gasperi).

Prof. dr hab. Józef Knap z Warszawskiego Uniwersytetu Medycznego w wykładzie *Cyberatak contra medycyna* precyzując terminologię z pogranicza technik informatycznych i medycyny, wyjaśnił, iż cyberatak to uderzenie na trzy sposoby: przeciwko pacjentom, czyli aparaturze wspomagającej, takiej jak respiratory, rozruszniki, inkubatory, pompy insulinowe; przeciwko urządzeniom medycznym oraz przeciwko informacji medycznej, czyli jej wytwarzaniu, gromadzeniu i prawdziwości, poprzez szantaż oraz atak w celu likwidacji czegoś. Infrastruktura medyczna wymaga zatem szczególnego rodzaju zabezpieczeń, których na ogół brakuje, natomiast cyberataki gwałtownie narastają. Kolejnym priorytetowym zagadnieniem medycznym była kwestia szczepionek poruszona przez **Izabelę Kucharską** – zastępcę Głównego Inspektora Sanitarnego Kraju. W referacie *Organizacja szczepień ochronnych w Polsce* została wyakcentowana konieczność obowiązkowego szczepienia wybranych grup, zalecenie szczepień ochronnych czy szczepienia dla osób szczególnie narażonych na skutek wykonywanego zawodu. Warunki te to bowiem sposoby osiągnięcia celów zdrowia publicznego, czyli osiągnięcia bezpieczeństwa populacji. Ewaluacja szczepień ochronnych wykazała zaś, iż uzyskano wysoki odsetek uodpornienia wśród populacji objętej programem szczepień ochronnych. Proces bezpieczeństwa zdrowotnego jest zaś wspierany przez takie nowoczesne narzędzie, jak Elektroniczna Platforma Gromadzenia, Analizy i Udostępniania Zasobów Cyfrowych o Zdarzeniach Medycznych.

Prof. nadzw. dr hab. Piotr Krajewski z Uniwersytetu Warmińsko-Mazurskiego w referacie *Dostęp do zasobów genetycznych i bezpieczeństwo epidemiologiczne* zwrócił uwagę na fakt, iż mimo niewątpliwych sukcesów ludzkość wciąż gnębiona jest nawrotami „starych" chorób i pojawieniem się nowych. Za szczególnie niebezpieczne – w kontekście bezpieczeństwa społecznego – uważa się oczywiście te zakaźne. Aby jednak skutecznie przeciwdziałać rozprzestrzenianiu się groźnych pandemii, czynniki patogenne powinny być udostępniane stosownie wyposażonym laboratoriom w celu opracowania skutecznych szczepionek i leków. I tu zatem istotną funkcję pełni informatyka służąca pomocą w opracowywaniu, kompletowaniu, przekazywaniu i gromadzeniu danych. Bez angażowania nowoczesnych systemów informatycznych sukcesy współczesnej epidemiologii nie byłyby możliwe. Z wykorzystaniem tych systemów wiąże się jednak szereg szczególnych i „typowych" dla tego obszaru zagrożeń i niebezpieczeństw, o których szeroko dyskutowano w trakcie tego spotkania.

Płk prof. nadzw. dr hab. Krzysztof Krakowski z Akademii Sztuki Wojennej w wielowątkowym referacie *Anatomia bezpieczeństwa według NATO w perspektywie 2030* przedstawił zmiany w architekturze bezpieczeństwa europejskiego, zwracając uwagę na to, iż przyczyniły się do nich takie współczesne wydarzenia, jak aneksja Krymu, konflikt rosyjsko-ukraiński w Donbasie, polityka zagraniczna Federacji Rosyjskiej, kryzys spójności Unii Europejskiej. Szczyt NATO w NewPort ukazał warunki, które musi przyjąć, aby wzmocnić swą solidarność. Należą do nich: obrona terytorium państw członkowskich, zwiększenie możliwości reakcji sojuszu, stopień gotowości dowództw, przeciwdziałanie zagrożeniom w cyberprzestrzeni, wzmocnienie sił w USA i Europie Północno-Wschodniej, zwiększenie wydatków na obronność. Niezwykle istotny w planowaniu nowej mapy bezpieczeństwa był warszawski szczyt NATO, w trakcie którego poruszono takie problemy, jak: finansowanie armii afgańskiej, problem szkoleń i tarczy antyrakietowej, nowi członkowie, wschodnia flanka NATO, wsparcie misji „Sea Guardian" oraz misja „Resolute Suport" w Afganistanie. Należy bowiem dostrzegać nowe trendy w środowisku bezpieczeństwa i reagować na takie, jak: globalne problemy demokracji, rosnące znaczenie Chin przy malejącej roli USA i spadku znaczenia Europy, widoczny sukces Rosji z jej wielokierunkową polityką zmierzającą do przy-

wrócenia mocarstwowej roli Rosji. Kontekstem polityki bezpieczeństwa jest zaś fakt ponownego wyścigu zbrojeń. Chiny o 9% zwiększają budżet na siły zbrojne, Hiszpania zaś wydaje na nie 15 miliardów dolarów, Polska natomiast przeznacza obecnie na zbrojenia 10 miliardów dolarów.

Konferencyjne tematy dotyczyły jeszcze wielu innych zagadnień. Temat priorytetowy to obszar etyki (**prof. dr hab. Bronisław Sitek**, Uniwersytet Humanistycznospołeczny w Warszawie; WSGE im. Alcide De Gasperi, *Etyczne granice stosowania nowych technologii informatycznych*). Etyka, obok mądrości, do której kilkakrotnie odnosili się prelegenci, to dwie fundamentalne reguły, zgodnie z którymi powinny funkcjonować nowoczesne technologie informatyczne w celu zachowania bezpieczeństwa obywateli, państwa i narodu.

W trakcie konferencji dokonano analizy obszarów, w których wykorzystywane są nowoczesne technologie informatyczne. Wśród owych newralgicznych obszarów można wymienić takie sfery, jak:

- zdrowie publiczne (**prof. dr hab. Jerzy Konieczny**, Uniwersytet im. Adama Mickiewicza w Poznaniu, *Technologie informatyczne w metodologii badań bezpieczeństwa zdrowia publicznego*; **dr Wacław Brzęk**, WSGE im. Alcide De Gasperi, *Kosmetyki a bezpieczeństwo konsumentów*);
- prawa człowieka (**prof. dr hab. Stanisław Sagan**, Uniwersytet Rzeszowski, *Nowe technologie inwigilacji w kontekście prawa do prywatności*; **prof. nadzw. dr hab. Magdalena Sitek**, WSGE im. Alcide De Gasperi, *Prawo do prywatności w dobie permanentnej inwigilacji*; **dr Krzysztof Krassowski**, WSGE im. Alcide De Gasperi, *Dychotomiczny konflikt wartości bezpieczeństwa i prywatności – czy prawidłowo stawiamy problem?*; **dr inż. Grzegorz Winogrodzki**, WSGE im. Alcide De Gasperi, *Informacja niejawna w cyberprzestrzeni – dylematy*; **dr Justyna Ciechanowska**, Uniwersytet Rzeszowski, *Zagrożenia dla bezpieczeństwa publicznego w kontekście prawa wyborczego*; **dr Robert Dębiński**, *Nadużycie prawa do wolności słowa i swobodnego wyrażania opinii, zagrożeniem dla bezpieczeństwa religijnego, narodowego i osobistego*);
- biznes (**Zsolt Tadeusz Fekete**, Algotech Polska sp. z o.o., *Liczby i trendy w biznesie cyberbezpieczeństwa*);
- administracja (**Grzegorz Poznański**, Ambasador Rzeczypospolitej Polskiej w Republice Estońskiej w latach 2010–2014, *Wpływ technologii in-*

formatycznych oraz wyzwań w dziedzinie cyberbezpieczeństwa na procesy podejmowania decyzji w administracji w obszarze bezpieczeństwa narodowego);

- ekstremizm islamski (**dr Magdalena El Ghamari**, Uniwersytet w Białymstoku/Fundacja El-Karama, *Nowoczesne narzędzia informatyczne w walce z ekstremizmem islamskim*);
- zagrożenia militarne, reagowanie kryzysowe (**dr Łukasz Roman**, WSGE im. Alcide De Gasperi, *Ewolucja zagrożeń militarnych w ujęciu polemologicznym*; **dr inż. Agata Szyran-Resiak**, WSGE im. Alcide De Gasperi, *Reguły działań public relations w zależności od typu sytuacji kryzysowych*; **dr Barbara Mróz**, WSGE im. Alcide De Gasperi/Komenda Główna Straży Granicznej, *Rola ćwiczeń reagowania kryzysowego w kształtowaniu bezpieczeństwa narodowego*);
- polityka (**dr Andrzej Wawrzusiszyn**, Uniwersytet Warmińsko-Mazurski, *Grupa Wyszehradzka wobec współczesnych zagrożeń transgranicznych*);
- kryminalistyka (**prof. nadzw. dr hab. Jarosław Moszczyński**, Uniwersytet Warmińsko-Mazurski, *Daktyloskopijne i genetyczne bazy danych – możliwości wykrywcze a praktyka*; **ppłk SG Dariusz Nawrocki, kpt. SG Norbert Grzmil**, Centrum Szkolenia Straży Granicznej im. Żołnierzy Korpusu Ochrony Pogranicza w Kętrzynie, *Cyfrowe źródła informacji wykorzystywane w analizie kryminalnej*);
- humanizm w cyberprzestrzeni (**prof. dr hab. Marek Lisiecki**, Uniwersytet Kardynała Stefana Wyszyńskiego, *Współczesne zagrożenia dla bezpieczeństwa obywateli*; **prof. nadzw. dr hab. Sławomir Zalewski**, Wyższa Szkoła Policji w Szczytnie, *Bezpieczeństwo obywateli w społeczeństwie informacyjnym*; **dr Sofia Sokolova**, WSGE im. Alcide De Gasperi, *Internet jako zasób nowoczesnej mitologii*; **dr Kateryna Novikova**, WSGE im. Alcide De Gasperi, *Bohater autentyczny a przywództwo oparte na wartościach: liderzy polityczni w wojnie informacyjnej*; **PhD Olena Hrybiuk**, Institute of Information Technologies and Learning Tools of the National Academy of Pedagogical Science of Ukraine, Kiev, *Variability modelling and the paradox of addiction in the context of the influence of social networks*; **PhD Galyna Biichuk**, Institute of Pedagogy of the National Academy of Pedagogical Sciences of Ukraine, *Information security of children on the Internet*).

Konferencja miała też aspekt szkoleniowy. Zaprezentowano zatem takie nowoczesne systemy, jak:

- **prof. dr hab. Ryszard Grosset, mł. kpt. mgr inż. Małgorzata Ciuka-Witrylak** *EvaCopNet – system wspomagający ratowanie poszkodowanych podczas klęsk żywiołowych z wykorzystaniem technologii zdalnego pomiaru parametrów życiowych*;
- **prof. nadzw. dr hab. Waldemar Zubrzycki**, Wyższa Szkoła Policji w Szczytnie, *Centrum Antyterrorystyczne ABW jako narzędzie w przeciwdziałaniu zagrożeniom terrorystycznym w Polsce*;
- **mgr inż. Adam Przybysz, mgr inż. Huber Nowak**, SARP/Transition Technologies S.A., *System Analiz Rejestrów Państwowych jako nowoczesne i bezpieczne narzędzie wspierania działań operacyjnych dla służb zapewniających bezpieczeństwo państwa i porządku publicznego*;
- **Maciej Iwanicki**, Inżynier Systemowy F5 Networks, *Chmura, aplikacje, bezpieczeństwo*.

Integralną częścią konferencji była projekcja filmu prezentującego potencjał edukacyjno-badawczy Narodowego Centrum Badań Jądrowych w Świerku, który może być inspiracją do dalszych analiz problematyki bezpieczeństwa w cyberprzestrzeni.